



AF  
JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

NCR Docket No. 9570

Application of:

FRAZIER, D.

Group Art Unit: 2134

Serial No. 09/897,628

Examiner: Andrew Nalven

Filed: July 2, 2001

For: PROVIDING SECURITY IN A DATABASE SYSTEM

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

APPEAL BRIEF TRANSMITTAL LETTER

Sir:

Transmitted herewith for filing is an Appeal Brief to the Final Rejection dated September 15, 2005.

- ☒ Please charge Deposit Account No. 14 0225 for the Appeal Brief fee or any other fees associated with the filing of said Appeal Brief.
- ☒ Please charge any additional fees to the account of NCR Corporation, Deposit Account No. 14 0225.

Respectfully submitted,

Harden E. Stevens, III  
Reg. No. 55,649

NCR Corporation  
Dayton, Ohio  
Tel. No. (803) 939-6505  
Fax No. (404) 479-1187

CERTIFICATION OF MAILING UNDER 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on 12/15/05.

By:   
Name: Michelle Hange

BEST AVAILABLE COPY



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: John D. Frazier

Serial No.: 09/897,628

Filed: July 02, 2001

For: PROVIDING SECURITY IN A  
DATABASE SYSTEM

§ Group Art Unit: 2134

§

§

§

§

§

§

§

§

§

§

Examiner: Andrew L. Nalven

Atty. Dkt. No.: 9570 (NCR)

Mail Stop Appeal Brief  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

BRIEF IN SUPPORT OF APPEAL

This is a brief in support of Applicant's appeal filed on October 17, 2005, in response to the final rejection dated June 15, 2005, in this matter. Applicant is filing this brief along with the required fee.

12/21/2005 DENMANU1 00000089 140225 09897628

01 FC:1402 500.00 DA

CERTIFICATION OF MAILING UNDER 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on 12/15/05.

By: Michelle G. Gaby

Name: Michelle G. Gaby

### **(1) REAL PARTY IN INTEREST**

The real party in interest in this matter is NCR Corporation, Dayton, Ohio, by virtue of an assignment recorded at reel 011991, frame 0977-0079, on July 2, 2001.

### **(2) RELATED APPEALS AND INTERFERENCES**

Applicant is aware of no active appeals or interferences related to this application.

### **(3) STATUS OF CLAIMS**

Claims 1-23 are currently pending. All of these claims are subject to a final rejection and are under appeal. A single claim amendment was made prior to this appeal. The word "accessed" was inserted into claim 17 after being inadvertently omitted. The text of the claims, as currently pending, is attached as an appendix to this brief.

### **(4) STATUS OF AMENDMENTS**

On September 15, 2005, Applicant filed a reply to the final rejection dated June 15, 2005. This reply contained no new amendments to the claims. In an Advisory Action mailed on October 6, 2005, the Office rejected Applicant's rebuttal arguments and maintained the rejection.

### **(5) SUMMARY OF CLAIMED SUBJECT MATTER**

In general, the invention provides enhanced security for data in a database system by providing "secure" data types (page 3, lines 11-13).

Applicant's claim 1 references a method requiring a user-defined data type (page 3, lines 11-13) and security information for the user-defined data type (page 3, lines 11-13 and fig. 2, element 102). Data is then stored according to the user-defined data type (page 3, lines 19-21 and fig. 2, element 104) and the security information is associated with the data (page 3, lines 17-21 and fig. 2, element 106).

Applicant's claim 5 references an article containing instructions executable on a database system (page 11, lines 14-17). The instructions cause the database system to provide a data type defining security information relating

to access rights and to store a instance of data according to the data type in the database system (page 5, lines 26-29 and fig. 1, TABLE A or TABLE B). The instructions further cause the database system to associate the security information with the instance of data (page 5, lines 26-29).

Applicant's claim 17 references a database system comprising one or more storage modules (page 5, lines 19-25 and fig. 1, element 28) used to store instances of data (page 5, lines 26-29). Each instance of data is accessed according to a secure data type associated with security information (page 5, lines 26-31). A controller determines whether or not to grant access to one of the instances of data in response to a query on whether the associated security information indicates that a source of the query has permission to access the one instance of data (page 5, lines 29-31).

Applicant's claim 23 references a database system comprising one or more storage modules (page 10, lines 5-6 and fig. 1, elements 10 and 28) used to store data instances according to a secure user-defined data type where the secure user-defined data type defines security information and one or more security functions (page 6, lines 5-11 and figure 2, elements 102, 104, and 106). A controller receives a Structured Query Language query originated by a source (page 2, lines 26-31 and fig. 1, elements 14 and 20) for one of the data instances and determines if the source is authorized to access the data instance based on the security information (page 10, lines 6-28 and figure 5, elements 202-218). The controller further invokes one or more security functions to process the data instance (page 10, line 29 – page 11, line 2 and figure 5, element 210).

## **(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

All claims stand rejected under 35 USC § 102(e) as being anticipated by Barkley (U.S. Pat. No. 6,202,066).

## **(7) ARGUMENT**

All rejected claims should be allowed over the cited reference for the reasons set forth below.

### **A. Rejection of Independent Claims 1, 5, and 17 by Barkley**

Barkley does not show or suggest “providing a user-defined data type,” as required by Applicant. The Office asserts that Barkley teaches user-defined data types in column 11, lines 20-25 where Barkley refers to “files related to depositor account information and employee information.” Applicant respectfully disagrees. A data type is a substantive programming construct. The American Heritage Dictionary defines the term “data type” as “a classification identifying one of various types of data, as floating-point, integer, or Boolean, stating the possible values for that type, the operations that can be done on that data type, and the way the values of that type are stored.” While this definition is too narrow, it never the less shows that a data type has structure and function which is consistent with Applicant’s description and use of the term. Applicant’s claim requires the presences of a data type that is just as tangible as data.

Barkley does not use the term “data type” nor does it teach the use of a “data type.” Furthermore, the mere presence of files that relate in some way to depositor account and employee information in no way implies the existence of a data type or that a data type was used as template to store data in these files. The cited passage is used by Barkley to illustrate his “role based” security system and how the role of an employee would govern their access to information. In this case, a bank employee would be given access to files related to depositor accounts but not to employee information. Barkley is not concerned with the details of the information, only the subject to which the information relates. Barkley does not teach a data type, or a data type that is defined by a user, or the presences of a data type. This required element of Applicant’s claim is missing from Barkley.

Barkley does not show or suggest “providing security information for a user-defined data type,” as required by Applicant. The Office asserts that Barkley teaches these elements in column 7, lines 20-40. Applicant respectfully disagrees. This passage teaches applying security information to objects and Barkley defines these objects as

directories and files (col. 7, lines 11-12). Applicant requires that security information be provided for a user-defined data type. Barkley does not teach a data type, or a user-defined data type, and he does not teach providing security information for a user-defined data type.

Barkley does not show or suggest “storing data instances according to the user-defined data type,” as required by Applicant. The Office asserts that Barkley teaches these elements in column 11, lines 20-25 where Barkley refers to “files related to depositor account information and employee information.” Applicant respectfully disagrees. Barkley never reveals the origins of these files and never gives any indication concerning how the files were created or their structure. It is possible that these files contain simple free form text with no structure at all. In any case, Barkley is silent on the issue. Furthermore, Barkley never teaches the presence of data instances, or a data type, or a user-defined data type, much less the use of a data type to store the data instances. These elements are missing from Barkley.

### **B. Rejection of Independent Claim 23 by Barkley**

The arguments made in subsection A above are applicable to this claim as well. In addition, Barkley does not show or suggest “a controller adapted to receive a Structured Query Language query,” as required by Applicant. The Office asserts that Barkley teaches these elements in column 7, lines 29-32 where Barkley states “the user is granted access to the objects according to the permissions mapped to the user ....” Applicant respectfully disagrees. Barkley does not use or teach the term “query” or the term “Structured Query Language.” Furthermore, the cited passage only teaches the granting of access. There is no mention of a controller or of receiving anything or any indication of what might be received. Barkley simply does not teach receiving a Structured Query Language query. This element and at least the elements describes about are missing from Barkley.

### C. Conclusion

Since all elements of Applicant's claim must be found either expressly or inherently in reference for a 102 rejection to hold, and since Applicant has shown that at least the above elements are missing, Barkley does not anticipate Applicant's claim. Therefore, the rejection is improper and the independent claims, along with the claims depending from them, are allowable over Barkley. Applicant therefore asks the Board to reverse the examiner's rejections and to allow all of the claims.

Please apply any charges or credits that might be due, except the issue fee, to the NCR Corporation deposit account number 14-0225.

Respectfully submitted,



Harden E. Stevens, III  
Agent for Applicant  
Reg. No. 55,649

NCR Corporation  
Law Department  
1700 South Patterson Blvd.  
Dayton, Ohio 45479

Tel. No. (803) 939-6505  
Fax No. (803) 939-5099

## **APPENDIX A - Current Listing of Claims**

**Claim 1 (original)** A method comprising:

- providing a user-defined data type;
- providing security information for the user-defined data type;
- storing data instances according to the user-defined data type; and
- associating the security information with the data instances.

**Claim 2 (original)** The method of claim 1, wherein associating the security information comprises associating the security information with each individual data instance.

**Claim 3 (original)** The method of claim 1, wherein associating the security information comprises associating an access list containing a list of identifiers of authorized entities.

**Claim 4 (original)** The method of claim 1, further comprising:

- providing one or more functions to perform predetermined one or more tasks for the user-defined data type; and
- invoking the one or more functions to process data instances according to the user-defined data type.

**Claim 5 (original)** An article comprising at least one storage medium containing instructions executable in a database system, the instructions when executed causing the database system to:

- provide a first data type defining security information relating to access rights;
- store an instance of data according to the first data type in the database system; and
- associate the security information with the instance of data.



Claim 6 (original) The article of claim 5, wherein the instructions when executed cause the database system to further:

receive a request to access the instance of data; and  
grant access to the instance of data based on the security information.

Claim 7 (original) The article of claim 5, wherein the instructions when executed cause the database system to provide the first data type by providing a user-defined data type.

Claim 8 (original) The article of claim 7, wherein the instructions when executed cause the database system to provide the user-defined data type by providing the user-defined data type in an object relational database system.

Claim 9 (original) The article of claim 5, wherein the instructions when executed cause the database system to store the instance of data by storing the instance of data in an object relational database system.

Claim 10 (original) The article of claim 5, wherein the instructions when executed cause the database system to further associate one or more functions with the instance of data, the one or more functions to provide one or more predefined tasks.

Claim 11 (original) The article of claim 10, wherein the instructions when executed cause the database system to further invoke at least one of the functions to add an identifier of an authorized entity to the security information, the authorized entity being authorized to access the instance of data.

Claim 12 (original) The article of claim 11, wherein the authorized entity comprises an authorized user.

Claim 13 (original) The article of claim 11, wherein the security information comprises a list of identifiers of authorized entities.

Claim 14 (original) The article of claim 11, wherein the instructions when executed cause the database system to further invoke another one of the security functions to remove an identifier from the security information.

Claim 15 (original) The article of claim 5, wherein the instructions when executed cause the database system to provide the first data type by providing the first data type defining one or more security functions to perform one or more predefined tasks.

Claim 16 (original) The article of claim 15, wherein the instructions when executed cause the database system to further provide a second data type built upon the first data type, the second data type inheriting the security information and one or more security functions of the first data type, wherein the second data type further defines one or more additional security functions.

Claim 17 (previously amended) A database system, comprising:  
one or more storage modules to store instances of data, each instance of data being accessed according to a first secure data type associated with security information; and  
a controller adapted to determine whether or not to grant access to one of the instances of data in response to a query based on whether the associated security information indicates that a source of the query has permission to access the one instance of data.

Claim 18 (original) The database system of claim 17, comprising an object relational database management system.

Claim 19 (original) The database system of claim 17, wherein the first secure data type comprises a user-defined data type.

Claim 20 (original) The database system of claim 17, the one or more storage modules to further store instances of data according to a second secure data type.

Claim 21 (original) The database system of claim 20, wherein the second secure data type is inherited from the first secure data type.

Claim 22 (original) The database system of claim 17, wherein each instance of data is further associated with one or more methods defined by the first secure data type, and wherein the controller is adapted to invoke the one or more methods to process instances of data according to the first secured data type.

Claim 23 (original) A database system comprising:

one or more storage modules to store data instances according to a secure user-defined data type, the secure user-defined data type defining security information and one or more security functions; and

a controller adapted to receive a Structured Query Language query originated by a source for one of the data instances, the controller adapted to determine if the source is authorized to access the one data instance based on the security information,

the controller adapted to further invoke the one or more security functions to process the one data instance.

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☒ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**